SYSTEM AND METHOD FOR NETWORK SECURITY

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] The present application is a continuation-in-part of United States Patent Application Serial No. 10/461,303 filed June 13, 2003, the entire disclosure of which is incorporated in its entirety by reference herein.

FIELD OF THE INVENTION

[0002] The present invention relates generally to information and more particularly to methods of information processing, which will make identity theft obsolete .

BACKGROUND OF THE INVENTION

[0003] Signatures have been utilized for centuries as the primary method of authentication. For many years, the process has involved a visual inspection between a newly signed document and a prior signature. This process, however, has significant limitations, as it typically depends on subjective decisions made by individuals having little skill, if any, in making signature comparisons. In recent years, computers have been increasingly utilized to assist in the authentication process, however, there are still significant drawbacks. Much of the problems have been a result of the increased globalization of business and society. For example, differences in language, culture and

geographic location have added many new variables that have needed to be considered and dealt with appropriately.

[0004] Another complicating factor is that we live, it is said, in the *'information age'*. What is meant by that phrase is that we live in a time when information is very important and easily accessible. To get a real appreciation, however, as to the impact the information age has had on society, it is necessary to reflect on the meaning of term "information" itself. "Information" is a term that has broad implications in today's environment and covers any type of "data" or "facts" and in any format, such as, for example, text, graphics, audio or video, to name a few.

[0005] Technological innovation has made it progressively easier in recent years to disseminate information from place to place, for example, by telephone, portable devices, such as recorders or PDA's, and via computer networks, such as the internet. The ease by which information can be readily obtained and disseminated have raised many concerns, such as privacy issues as well as issues of fraud and security concerns. Laws have been enacted in attempt to deter piracy of sensitive public or private information, but that has done little to address the source of the problem.

[0006] Moreover, as technology advances and links goods and services throughout the world, the economy and stability of civilized societies become more vulnerable to sophisticated means of attack and destabilization. Government and businesses are linked world wide via telephone, cable, and wireless technologies. This technological communications revolution has left our society open to a new worldwide threat. Interference with our current technologies by a third party wishing to cause chaos in the free world is a constant and real threat to all people.

[0007] The computer linked worldwide communications systems are vulnerable based on the current system. The present system allows acceptance of devastating electronic programs such as so called "worms" and "viruses". The present system also allows the very worrisome intrusion by "hackers", who can gain control of vital government functions and an individual's personal records.

[0008] Apart from prevention of attacks upon the information that is linked to government and private institutions, a method to track and help apprehend the criminals and terrorists that wish to harm the free world is also needed. Presently, there is no system in place to link the actual person responsible for the attack to the crime.

[0009] In view of the forgoing, there is seen a need for improving the manner by which information integrity can be maintained and dissemination regulated.

SUMMARY OF THE INVENTION

[0010] The present invention discloses a system and method for network security.

[0011] In accordance with one embodiment, a method comprises the steps of storing information in a memory device and regulating access to the information stored in the memory device based upon a security measure. In an exemplary embodiment, the security measure may comprise one or more biometric characteristics. The method may further comprise one or both of the steps of providing a reader to regulate access to the information stored in the memory device and providing an interface to communicate with the reader or memory device upon permission to access the information. The method

may also comprise the step of identifying the location of the memory device at desired times.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] The present invention can best be understood in connection with the accompanying drawing, in which:

[0013] Fig. 1 is a block diagram illustrating an exemplary embodiment of the present invention.

[0014] Fig. 2 is a block diagram illustrating another exemplary embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

[0015] The following embodiments of the present invention may be implemented using hardware or software or any combination of the two where desired. Various embodiments may also be implemented using commercially available technology.

[0016] In one embodiment, a method for processing information comprises the steps of storing information and regulating access to the information based upon a security measure. In an exemplary embodiment, the security measure may comprise one or more biometric characteristics, which is described in further detail below, although it should be understood that any desired security measure may be utilized where desired.

[0017] In order to illustrate the foregoing method, the following example is provided comprising a storage device 12, such as an identification memory card, a processing device 14, such as an identification card reader, and an interface 16, such as a host device, as is illustrated in fig. 1.

[0018] The term "storage device" as used herein should be broadly construed to comprise any device that includes the capability of storing information, such as via any suitable electronic or magnetic storage medium adapted for storing information in digital and/or analog form. The term "identification memory card" should also be broadly construed to comprise any storage device suitably sized and configured so as to be portable. For purposes of illustration, the following examples are described in relation to one embodiment of an identification memory card comprising a smart card type of device, such as a Digital ID™ ("DID™") card, which is preferably sized and configured corresponding to a conventional credit card and includes memory and processing capabilities to store and process information in digital form. It should be understood, however, that the identification memory card may comprise other sizes and configurations where desired as well as store and process information in other formats, such as analog and/or magnetic, to name a few.

[0019] The term "processing device" as used herein should be broadly construed to comprise any device having the capability for communicating with the storage device and interface described herein and for processing information relative to these devices where desired. The term "identification memory card reader" as used herein should also be broadly construed to comprise any suitable type of processing device capable for communicating with the identification memory card and host device in accordance with

embodiments of the present invention, such as is illustrated in fig. 1 and described in detail below.

[0020] The terms "interface" and "host device" as used herein should be broadly construed to comprise any suitable device adapted for communicating with the processing device/identification memory card reader and/or the storage device/identification memory card, where desired. For example, the host device may comprise a separate device, such as a computer or telephone or any other suitable device, capable of interfacing with the identification card reader. This interface may be accomplished by any suitable, means, such as via standard Serial, USB, or IEEE-1394 "firewire" computer interfaces. In other embodiments, the host device and identification card reader may comprise a single device. Application software may run on the host computer for any number of given services, such as commercial transactions, medical records, travel documents, entertainment transactions, government administrative documents and the like. Each service may have distinct application software as well as a unique identification reader/sender associated with it for reading and transacting the transactions of the identification memory card. The host computer gains access to the identification card data through interface with the identification card reader, which in one embodiment includes a user-specific biometric keying device on it. The identification card reader sends the biometric data to the host computer for later processing and comparison. The reader may be unique for other applications. Different applications may access different encrypted areas of the identification card's secure memory where desired.

[0021] The terms "computer" or "server" as used herein, include any device capable of receiving, transmitting, and/or using information, including, without limitation, a processor; a microprocessor; a personal computer, such as a laptop, palm PC, desktop or workstation; a network server; a mainframe; an electronic wired or wireless device, such as for example, a telephone; an interactive television or electronic box attached to a television, such as for example, a television adapted to be connected to the Internet; a cellular telephone; a personal digital assistant; an electronic pager; and a digital watch.

[0022] As will be described in more detail below, in accordance with various embodiments of the present invention, information may be transferred between the storage device/memory card 12 and one or more locations external to the storage device/memory card 12. The term "one or more locations" should be broadly construed to comprise any designated location that is desired to interact with the storage device/memory card 12, such as an institution as an example, as is discussed below. The one or more external locations may include one or more databases or similar types of storage devices capable of interacting with the storage device/memory card 12 by uploading and downloading of the information.

[0023] Information may be transferred between the storage device/memory card 12 and the various external locations via the processing device/identification memory card reader 14 and/or interface/host device 16, for example, over any network. The term "network" as used herein with the various embodiments should be broadly construed to comprise any wired or wireless network, or any combination wired/wireless network, such as, for example, a telephone or cellular telephone network, an internal business network,

cable/DSL/T-1 networks, satellite networks, the Internet or world wide web, an intranet, or an extranet, etc.

[0024] In one embodiment, for example, although others are applicable as well, the reader may have a configurable contact arrangement that provides for each reader being unique for a given application. In this way, different readers may be needed for access to different areas of the identification card memory. The identification card reader may contain an AC or DC power source and a controller interfacing with the identification card. Furthermore, location tracking may also be incorporated into the overall system where desired. For example, the reader may be equipped with required front end RF and conversion needed to support a single chip receiver and a global positioning system(GPS) processor in the identification card.

[0025] In another embodiment, the identification card may contain a configurable contact arrangement that is decoded for access to the secure memory of the identification card. In this way, application data contained in the memory for one purpose preferably will not be accessed by another unrelated application intended for another purpose. For example, a provider of medical records cannot have access to commercial banking records, and vice versa. In this manner, access to the data is restricted and tailored for one use or another. Identification card memory may be segmented by each application area. Each area may also be assigned a designated capacity space for storage. These information areas may include, but are not necessarily limited to, one or more of the following examples: encrypted data of an identification card carrier, photographs, medical history, credit card information, dental records, driver information, credit card records, immigration documents, travel and passport records and general personalized data, etc.

Furthermore, the identification card may be equipped with a global positioning system capable device that may be powered from the identification card reader where necessary. An RF feed may be utilized when the device contained on the card, such as an onboard processor, cannot receive energy from an onboard antenna.

[0026] An exemplary embodiment may be used as a digital identification device. The digital identification device may comprise a card or like type of device that may be utilized as a secure personal information medium. In this embodiment, non-removable, non-volatile solid state memory, such as flash memory, may be used to store encrypted digital data in the record unit, although other storage mechanisms may also be utilized where desired. The memory may be partitioned and adapted to store specific data types in specific locations in the memory. In this way, memory blocks may be assigned to information areas such as, for example, personal name, encoded digital individual identifying photograph, medical history data, driver's data, etc. The card may also have a connector, such as along its bottom surface, which interfaces with a separate reader, such as a playback/send reader unit, when the card is inserted into a recessed port, such as in the reader's top surface. The playback/send unit may also have a unique pin code, which allows access to the specific data encoded on the digital identification memory card. In this manner, only specific users can gain access to specific data, making the card unalterable by others. For example, it can be regulated so that the individual who is issued the card, i.e., the owner of the card, can not access the data to tamper with or change any information, police can access the Picture ID and driver's data but not the medical or other personal data, likewise a doctor can access the medical history but not bank records, etc.

[0027] As indicated earlier, a location tracking mechanism, such as a single chip GPS engine or any other suitable device, can also be included as a part of the overall system and method. In one embodiment, when connected to the playback/send unit, an electrical path is created that connects the Antenna on the playback/send card reader unit to the single chip GPS solution. Power is then applied via the playback/send unit. Upon power-up and a time delay needed for the GPS signal to be processed, time and location information is available. This location and time information may also be used to time stamp designated or every transaction in the digital identification card. Furthermore, the playback/send unit may also contain a biometric fingerprint reader that allows correlation from user to stored biometric information on the card. Only a correct match will allow access to data on the card.

[0028] Another embodiment comprises a digital identification memory card with Wireless connectivity. In this embodiment, the digital identification memory card may be mated with wireless transmission capability. In this embodiment, the digital identification memory card may be enhanced with microprocessor, RF receive, RF transmit and a power source, such as a battery. This capability allows for connectivity to wireless LAN as well as the Internet via wireless Internet connection. Reception and decoding of the (GPS) enables the card to locate itself. In this way the location of the card can be broadcast, received and shown on a map using a standard Internet browser. Also short messaging service (SMS) or enhanced messaging service (EMS) or other text messages can be sent to a wireless mobile handset upon request of authorized user. In this embodiment, the playback/send unit may also operate as a battery charger.

[0029] In another embodiment, a location device can be provided on the memory card and may communicate by wireless means with a reader in the form of a scanner, when the card is brought into proximity with the scanner. For example, the location device can be adapted to transmit designated information, such as an ID, to the scanner either automatically or upon request of the scanner. The location device may be powered by either a source external the card, such as by the scanner, when the card is brought into proximity with the scanner, or by a power source located on the card itself. In this embodiment, the location device may be adapted to communicate with the scanner from various distances, such as directly next to one another, i.e., 0-1 foot or from larger distances, such as the size of a room or building or a complex, etc. The scanner may further process the information received from the card in any desired manner. For example, the scanner may be utilized as a counter, such as to count the number of passerby's, such as for use at stores, conventions, trade shows, etc. In addition, the scanner may compare the ID against designated information, for example, an allow/deny list, most wanted list, etc. The designated information may be stored local at the scanner or provided from an external storage source, such as via a network connection. The scanners may be located at various pre-selected locations, such as at border check points or other secured areas, and in radar or other law enforcement equipment, etc.

[0030] Still another embodiment is utilized as a personal digital voice recorder for persons, including but not limited to medical patients and children. In this embodiment, the recorder stores real time voice data, such as non-volatile memory. Recording may start at any desired times, such as by a parent, utilizing the playback/send unit. The recorder may then be attached to a user, such as a child or patient, and all proximity

sound to the child or patient is recorded until either a low power condition or a memory full condition is reached. The memory may be scalable according to the amount of recording time and fidelity desired by the parent or authorized custodial person.

[0031] Another embodiment may be utilized as an automatic voice notebook, such as for health care professionals on rounds as an example. Similar uses, such as by building inspectors, maintenance or security and Military personnel, as an example, are also anticipated. In this embodiment, memory, such as non-removable, non-volatile memory, such as flash memory, may be used to store encrypted digital data in the record unit. A small cell may be used in this unit to keep size and weight to a minimum. A real-time clock may be embedded in the record unit to be used for time stamping the recorded voice segments. The record unit may have a connector, such as along its bottom surface, which interfaces with a separate playback unit, such as when the record unit is inserted into a recessed opening in its top surface. The playback unit may include conventional features, such as speaker, play button, volume control and "forward/reverse" switch for navigating within the data. Both the record unit and the playback unit may further have identifying features, such as matching bar codes on their housings, which can be used to identify the individual units in case of loss or to confirm identity.

[0032] A further embodiment pertains to a method and system of authentication and tracking of the personal originator of electronic files. This method enhances security and provides accountability for files such as electronic mail and electronic commercial documents to name a few. The unique personal identifier such as one or more biometric parameters are used in place of a traditional signature or written mark. This method utilizes new technology that makes use of a compact portable electronic storage device,

unique identifying personal markers, such as biometrics and other personal characteristics, special tracking circuits with global positioning satellite technology, software, and any internetworking or linking of communication devices such as computers, PDA's cell phones, etc. This method further utilizes a designated unique reader to interpret the digitized data and authenticate the data by using one or more biometric sensors. This method also provides for a unique identifying mark visible "on the outside" of the file that verifies the identity of the sender of the file before the file is opened and potentially downloaded onto the recipients hard drive. The method thus allows for personal authentication and accountability as well as the exact place and time of file origination. Some exemplary advantages and embodiments of this method are listed below.

Security- the originator of the file is identified. Forgery and fraud utilizing electronic documents can be eliminated. This applies to all aspects of business including commercial and government.

Safety- the authenticated signature is visible without opening the electronic file. This method allows individuals, businesses, and government to automatically reject all files without an external authentication mark. This will make passing and spreading of harmful electronic programs such a "worms" and "Viruses" much more difficult.

Location-this system allows for location tracking either in real time or by specific event. This is done using GPS technology and software. Not only can the location be generally discovered but the exact place, time , and person can be

discovered and brought to justice. Specific areas and people can be watched by authorities more closely and apprehended.

Privacy- this method allows the individual to chose what files are sent to his or her computer or device. This will effectively regulate "spam" and the invasion of an individual's privacy.

Example A -Home Use

[0033] User I --- DID™ Card placed in reader "HOME USE"--- fingerprint and/or retinal scan confirmation confirms identity ----- electronic file is written and sent from "HOME" computer ------ Recipient computer receives electronic file into IN BOX---User 2 opens computer and views IN BOX ----- User 2 identifies an "AUTHENTICATION MARK" verifying the identity of the sender ---- User 2 opens the file and reads content safely and securely.

[0034] The procedure may be utilized over any computer network, such as the Internet. In addition, the procedure may be utilized in a similar manner for any person to person or multiple party communication in real time, such as instant messaging or chat room communication.

[0035] Alternatively, User 2 may pre-program his computer to only allow "Authenticated" signed files. This will automatically block most "spam" before it reaches the IN BOX. This protects the individual's privacy.

Example B- Illegal Activity

[0036] User I ------ logs onto internet without secure authentication------ sends file with a new virus to GOVERNMENT or BANK computer------- Recipient computer software checks for Authentication Seal ------ No biometric seal is indicated ------ file automatically deleted------ return message to computer originator stating no personal authorization so file was deleted without being read.

[0037] This example demonstrates a security level to help protect business and government files from attack by viruses, worms and hackers trying to hide their identity. The integrity of the organizations computer network will be safer.

Example C - Identifying and Tracking Wrongdoers

[0038] User I ------ DID™ Card placed in reader------ biometric sensor verifies ownership using fingerprint and or retinal scan for example----- time and place stamped via GPS chip-------electronic file with NEW VIRUS is created and sent to bank------ bank computer opens file and becomes infected------- User 1 is identified as John Doe residing at 123 Smith Lane Hollywood California 99201. The file originated at (exact location and time and date) ------ the bank blocks all further email authenticated from User 1 biometric signature------ the authorities quickly find and arrest the wrongdoer------- his DID™ Card documented the transaction and is used as evidence in his trial. Similarly, the system can be utilized to prevent child pornography.

[0039] In an alternative version, the DID™ Card can be real time tracked via GPS and the criminal located faster.

[0040] In a further embodiment, the memory card may be utilized as a means to conduct various financial transaction, such as cash withdrawals or transfers as well as check or credit card transactions, to name a few. For example, in a cash transaction, the memory card may be utilized to reach a designated banking institution, such as over a network, for instance, the Internet, to electronically transfer funds from a specified account so as to be downloaded and stored on the memory card. In this embodiment, the memory card becomes, in essence, a secure wallet. Funds may also be transferred from other institutions or individuals to a particular memory card.

[0041] In a similar manner, funds may be transferred in the opposite direction from a memory card to a designated financial institution, such as for deposit, or to some non-financial institution or an individual, such as for a purchase or payment.

[0042] Also, in a check transaction, the same process can follow in that a check may be stored on the card, and when connection is made to a designated institution, the checking information may be uploaded from the card and download at the institution, such as for deposit or to make a purchase or payment by check, or the transaction may be for check cashing, in which the further step may occur of funds in electronic form being transferred from the institution and downloaded onto the card.

[0043] In the present embodiment, since funds are transmitted and received coded according to a biometric, individuals, government and businesses may freely distribute funds over the Internet, such as employee payroll. In addition, should an owner ever lose or misplace his or her card, any funds that may have been be stored on that original card are not lost. A person finding the lost card can not access the funds, since there will not

be a biometric match. The same funds can then be provided on a new card by the bank, institution or party that issued the funds originally. The original funds that were issued may also be voided where desired.

[0044] Another embodiment in accordance with the present invention pertains to signature verification. As is illustrated in Fig. 1, an exemplary embodiment comprises a storage device in the form of a memory card 10, a processing device in the form of a reader 12 and a host device in the form of a computer 14. As indicated above, in other embodiments, the reader and computer may be combined together in a single device where desired. Other processing devices may utilized as well, such as fax machines, etc. In this embodiment, the memory card 10 and an associated security measure, for example, biometric information stored on memory card 10, may be utilized to verify identity. The memory card 10 may be used in combination with one or more biometric characteristics taken from the user for the purpose of signature verification. The following illustrate some examples in accordance with the present embodiment.

[0045] In one example, .the memory card 10 and biometric match may be required of a user in order to gain access to a designated device, such as to log onto a given computer. The memory card 10 and biometric match would in essence serve as a password in this embodiment to verify the identity of a user. Access may be denied where a user's identity is not verified. In other embodiments, access to any given computer may be restricted to designated individuals, so that the memory card and associated biometric information would also serve to limit access to only permitted users.

[0046] In addition, in accordance with this and other examples, the memory card 110 and biometric match may be required of a user in order to communicate with a recipient, such

as electronically over a network, for example, by email, a digital sender, fax or other document in electronic form. As indicated above, where the memory card 10/biometric match is required to log onto a computer, then identity has already been verified and further security measures in order to communicate with a recipient electronically may be optional where desired. Alternatively, if there are no log in security measures or for added security, an electronic communication may further require an authentication mark, to verify the identity of the sender, which may be packaged with a communication sent to a recipient.

[0047] The authentication mark in accordance with the various embodiments may be utilized so that it is either visible to the recipient or not, as may be desired. A visible authentication mark, as indicated above, may serve as a signal to a recipient that it is safe to open a document. The presence of the authentication mark, however, irrespective of it being visible or not, may serve as a mechanism for signature verification, as discussed below. The system can be set up, for example, so that a communication will not be sent from a particular computer and/or will be refused receipt by a recipient computer unless an authentication mark is present. Alternatively, it can be arranged so that the sender and/or recipient computers are able to detect the presence of an authentication mark, and then notify the recipient whether or not one exists. Other examples are also possible.

[0048] An authentication mark may include a variety of designated information regarding the sender, such as name and location. Location information may be provided via the computer 14, such as a particular internet protocol("IP") address. In other embodiments, location information may be provided by other means, such as via memory card 10, for example, GPS tracking information may be uploaded from the card 10 to the computer 14

via reader 12. Biometric and/or Name information may be provided from the memory card 10. Other information may also be provided as well where desired, such as time and date stamp from either the memory card 10 or computer 14 or both.

[0049] In a transaction, the authentication mark serves to verify the identity of a sender of an electronic communication, and accordingly, may also serve to authenticate the content of a particular electronic communication. For this reason, the authentication mark may function as a form of signature verification or as a substitute for a physical signature, such as in situations requiring a signature to be binding, for example, legal documents, such as contracts, financial transactions, business transactions, etc.

[0050] In another embodiment, one or more servers or other interfaces may be utilized as a gateway for any desired communications over a designated network. For purposes of illustration, shown in fig. 2 is an exemplary embodiment comprising a processing device 210, such as computer at a first destination, in communication with a server 212 via a network connection 214, such as the Internet. The server 212 is, in turn, in communication with one or more further processing devices, such as a computer 216 at a second destination.

[0051] As will be described in more detail below, communication between the respective computers 210 and 214 may be routed through server 212 for security purposes. For instance, a security measure, such as an authentication mark discussed above, can be utilized that is sent from a designated computer and routed to server 212 for verification purposes. In one embodiment, the security measure may comprise any biometric information in electronic form, such as fingerprints, of the sender. The biometric information can be obtained in a variety of ways, such as from a memory card or directly

from the sender prior to a transaction. The server 212 can conduct a comparison of the biometric information received from the designated computer against stored biometric information, such as contained in a database(s) local at server 212 or some external location. Other information can also be stored in the database(s), such as levels of security clearance of designated persons. Depending on the results of the biometric comparison, further processing can be regulated. For instance, if no biometric match is made, then authorization may be denied in order to access other designated computers. Other controls can be similarly implemented.

[0052] In one exemplary embodiment, where an electronic communication may be desired to be sent from computer 210 to computer 216, a biometric security measure may either be packaged with or sent associated with the electronic communication (i.e, substantially at the same time or before/after) and received by server 212. A biometric comparison is then conducted at server 212, such as fingerprints mentioned above, although as should be understood, any other biometric information may also be used as well. Based on the biometric comparison and/or presence or absence of any other data stored in the database, the electronic communication may either be routed to the destination computer 216, if authorized, or routed to some other destination or retained at server 212, if not authorized. As mentioned above, other information capable of being stored in the database may include various levels of security clearance associated with authorized persons, so as to regulate access possible depending on the sender. For example, the security clearance level can control which designated computers the sender will and will not be granted permission to access. For instance, persons designated with the highest security clearance level may be provided with full access, and those persons

with less than full clearance may be provided with various restrictions, depending on the individual persons particular security level.

[0053] Further, the server 212 may also be utilized to detect the presence of any viruses, worms, etc associated with the communication, and then similarly route any problem communication to designated locations other than computer 216 or retained at the server 212. In addition, where any problem is detected, the sender's biometric information may also be forwarded to authorities where desired for identification purposes.

[0054] The foregoing system may be utilized where ever desired, and in particular, where ever network security may be a concern, such as, for example, the internet or world wide web, any internet providers, government agencies, financial institutions, databases containing any sensitive company or personal information, or any other public or private networks, etc. The system preferably utilizes a gateway(s) so as to regulate communication over these various networks. The gateway itself operates by being associated with various security measures. The security measures can include, for example, biometric information of authorized (and/or unauthorized) persons and a level of security clearance, as mentioned above. It should be understood, however, that other security measures may also be utilized where desired.

[0055] Advantages of the system of the present embodiment include that it can be adapted for a variety of different applications and implemented to existing networks with little, if any, change in infrastructure. Some examples of the many applications include to regulate communication over the world wide web or Internet, such as by identifying individuals as subscribers of particular internet service providers, or as employees of particular corporations or government agencies, etc.

[0056] In still another embodiment, a memory card can be used to verify identity of an individual in situations where merchandise or services owed to that individual is desired to be received, such as will call transactions.

[0057] Some examples of the various advantages of certain embodiments of the present invention include:

1. Configuration – a storage device, despite its complexity of microchips and printed circuit board interconnections, is configured into a lightweight device, such as a card that can be easily stored in a wallet.

2. a storage device does not require a battery for its operation.

3. Security – data entered via contacts or pins is encrypted and stored. Outgoing data is then decrypted. This can only be done if the contact reader is classified as a reader for that specific data.

4. All data is partitioned or compartmentalized so only certain readers (also referred to as playback/send units) can have access to certain data. For example, if this device were used as a driver's license, a police reader would have access to the digital photo, driving record, arrest or conviction record of the driver.

5. No data can be transferred unless there is a biometric match between the reader (playback/send unit) and the person who possesses the card – such

as fingerprint or fingerprints, palm or hand print, retinal match, face print, or DNA screen, as examples.

6. A digitally encrypted picture of the owner of the card.

7. Data from the card is automatically stored in the hard drive of the card-issuing establishment and can therefore be easily replaced by uploading using special software.

8. Ruggedized for protection of internal circuits and microchips.

9. Integration of location tracking technology, such as GPS technology with unique circuitry allowing for exact placement of the card in time and space when it is utilized. This feature can have widespread implication, such as in preventing crime or fraud in multiple industries.

10. Interactive nature – a storage device can be edited as well as unedited. The advantage of this feature is reflected in this example: A person visits a doctor. The person presents his card. He or she is biometrically linked to the card so ownership is verified. His or her insurance information and medical information from his or her last encounter with any physician is recorded, as is the time and place he or she was seen. The doctor examines the patient, updates the card through the physicians send/play

back unit and writes the patient a new prescription (special software can further assure that the prescription does not interact adversely with other medications the patient is presently taking, can also inform whether the drug is covered by his or her insurance company, and can clearly print the name of the mediation and instructions). The patient then goes to the pharmacy. He or she is again identified via biometrics, his or her card is placed in the pharmacy reader. The pharmacy reader cannot read other information about the patient except items permitted to access. This will primarily be insurance information and the prescription information. This is one example of the interactive nature of the card, although as should be understood, other examples may also be provided.

The interactive nature of the identification card in accordance with embodiments of the present invention may provide any number of the following advantages:

- Identification protection through encryption and/or biometrics.
- Confidentiality by the partitioned memory and contact system of the play/send functions to allow only information needed for each transaction.
- Unique ability to edit based on access to certain portions of the system by certain readers.
- Security – no one reader can read all portions of the system

- Reduction in medical error – the information on the patient's exam is accessible to all medical specialists in different locations all over the world. The time and place stamp helps with the accuracy and decreases the doctor's need to rely completely on patient recall, which leads to better care and markedly reduced costs to the medical industry (less duplication of test, etc.). Further, prescription error will be eliminated saving lives and money.
- Insurance Fraud – people cannot use other people's cards, having enormous implications in Medicaid fraud and health insurance fraud in general.
- Prescriptions can be linked to what the insurance formulary will cover – this allows both pharmaceutical and health insurance companies to same money.

11. An identification card may be uniquely treated so that it is resistant to elements and routine mechanical stress. An example of this is flame resistance, water resistance and bend resistance.

12. Contact as well as adaptation to contactless operation between the card, reader and host device.

[0058] Some further examples of advantages of still other embodiments of the present invention include:

1. Power source included in the card, such as alkaline, nickel, lithium battery or solar cell, as examples.

2. Location tracking added.

3. Mechanism for emergency contact, such as an E911 feature – this may be a contact feature or a voice recognized feature, as example, responding to words such as "help".

4. Integration capability of Wi-Fi technology to adapt the product through circuit integration to a local area network in a defined region, some examples include blue tooth and 802.11.

5. Integration of digital images through lens and voice transfer through microphone/speaker adaptability.

[0059] In accordance with the various embodiments of the present invention, the following is a partial listing of some exemplary application areas:

- Police and Law enforcement.
- Insurance Industry, including healthcare.

pharmaceutical formularies, Medicaid, Medicare, etc.

- Medical – Dental records.
- Financial such as credit cards, debit cards, bank cards, etc.
- Hospitality – such as travel and loyalty points.
- Immigration such as student visas.
- Government – social security card, homeland security card.
- Corporate.
- Individual and Privacy Identity Protection.
- Entertainment.
- Personal use.

[0060] In addition, embodiments of the present invention may further include a memory device, such as a stick/chip, which may only record and not have an audio or playback feature directly incorporated into the unit. The separate and detachable memory stick may be programmed to record and document any disruption or removal from the system including logged in and logged out times and dates. Also, the memory stick can have a code that does not allow any changes to be made to the recorded voice without using a unique code, such as, for example, a 12 digit code accompanying the original unit. This will prevent tampering and allow proper documentation of originally recorded voice data. In other embodiments, the memory device may be incorporated within the identification card itself.

[0061] The following illustrates in more detail some of the exemplary application areas in accordance with the various embodiments of the present invention.

1. Homeland Security:

The following describes one exemplary embodiment in relation to homeland security. In this embodiment, a foreign national enters the United States(or similarly, some other country) and is issued an identification memory card. The card may be encrypted with a digital photograph and other unique identifying biometric data, such as a fingerprint. The entry is permanently time, date and place stamped by indisputable GPS chip in the card. This card can be tracked in real time or traced with each use. Uses in cards for student visas, visitor visas, passports, etc., can be utilized with this technology. The legal record for this individual can be entered into the card, such as the purpose here in the U.S. and who the immediate family members are, etc. This information may be seen only by the proper legal authorities, such as the police, INS, etc. No one else can use the individual's card because of the biometric utilization features. Without the fingerprint, for example, the card is useless and cannot be read. An individual is linked to a particular card. The card may also be tracked where desired. If someone is being sought for illegal activity, as an example, the card will locate them via GPS. If they have discarded the card and are apprehended with someone else's card, the biometrics will not match. If they do not have any card, or a proper card, then their biometric data will reveal their true identity.

Law enforcement will have biometric readers that are part of the system to help in this process.

Furthermore, in other embodiments, cards may be utilized as a social security/homeland security card. These cards can provide accurate information that preferably cannot be altered with the exception of authorized government agencies that issue the data. The biometric link to each card verifies the individual of the card as owner and can place the owner at a specific location, date and time. This system provides an unprecedented level of personal identity security and protects society from imposters and criminals wishing to cause harm by using deceitful practices. The social security number for each person can be digitally encrypted and protected by multiple levels of biometric security. This will virtually "identity theft proof" the card. Individuals may also choose if they want the card to be trackable in real time to help them locate it if lost. The universal applications will encourage people to want to have a single memory card as opposed to a wallet full of separate conventional cards.

2. Law Enforcement:

The identification card can also be utilized as a driver's license. The added features can include information such as outstanding tickets, prior arrests, etc. Biometrics assures the identity of individuals to authorities. The owner of the card benefits by the secure nature and unalterability of the card. The owner also benefits from the universal applications, one of which will include the insurance information and car registration stored on the card. This will also help

in eliminating the possibility that individuals will be issued citations for not having these cards available.

3. Healthcare:

One feature of the memory card, besides the safe transfer of medical records and dental records, including x-rays, is fraud prevention. A medical provider may not be able to commit fraud by stating a patient was treated that was not treated since the biometrics and time/place stamping offered by GPS clearly shows the patient was in that location at that time. Further, a health insurance card such as Medicaid or Medicare card cannot be used by anyone but the owner of the card. This will help to prevent unauthorized persons such as unregistered illegal aliens from illegally gaining access to the Medicaid or Medicare system. It will also prevent the illicit receipt of prescription medications. It will ultimately prevent anyone but the authorized owner of the card to derive any health or medical benefits from the card.

4. Financial Transactions:

The memory card can be utilized for electronic transactions, including, for example, credit card, debit card and ATM features. Examples would be similar to how these stand-alone cards are used today with a major exception. Personal biometric data is presented at the time the card is used, which will eliminate credit card fraud and theft. For example. no transaction can take place with the card, such as at a department store check-out register, unless the biometric indicators

are matched, such as fingerprint. Further, as discussed above, the manner in which the card is designed in certain embodiments will not allow other compartments to be viewed. The reader will only be able to access/verify needed information for the transaction. This might include a catalog of credit card numbers to be chosen from, a photo ID and fingerprint verification, as example. For illustration purposes, pins 1 and 3 are attached to the reader and interfaced with the card, allowing display of the data onto a computer screen, register screen, or handheld reader with LCD. The transaction is permanently time/location stamped by the card itself.

5. Privacy:

One of the features of the memory card in accordance with embodiments of the present invention is privacy. No one place or establishment has access to all the identifying information. A merchant or other third party will only have access to designated information. The remainder of the information is protected. The information may also be date/time stamped for added protection as well as tracked where desired.

Depending on use, a memory card may be tracked by an individual and not necessarily any organization. This may be done via a cellular/satellite network and corresponding Internet website. An aspect here is the ability to compartmentalize the data and its use. This allows one card to be used for all features and privacy to be maintained.

[0062] The following is another exemplary embodiment of the present invention. In this example, Baby Jane Doe was born on June 2, 2003 at 2:00 AM EST. at Winthrop Hospital in Mineola NY. Her physician signed her birth certificate, which was forwarded to New York State for processing. The nurse in the hospital used special ink to mark her hand prints and footprints for the proud parents. A copy was also forwarded to the Social Security Administration. The Social Security Administration issued Jane Doe a card called the DID™ Card.. It is a specialized memory card that will be with Jane Doe for the rest of her life. It will store her biographical and biometric information. It will protect her from being the victim of fraud and identity theft. It will help keep her information private as she grows into an adult and through the many facets of the life ahead of her. This new card will help protect her health. It will help prevent medical errors. The card will enable doctors to treat Jane Doe with greater accuracy. It will also help Jane Doe save tens of thousands of dollars over the course of her life. The following illustrates the possible uses of the DID™ card over Jane Does' lifetime.

[0063] Jane Doe receives her DID™ card two weeks after she arrives home from the hospital. The DID™ card is preloaded by the Social Security Administration(SSA) with the following information. Name, address, date of birth, SS#, digitally encrypted picture, Digitally encrypted hand print(all of this information can not be edited, erased, rewritten, tampered with or reproduced except by the SSA), digitally encrypted photo of both parents as well as parents fingerprints and retinal print. The remainder of her card is empty storage which will be filled throughout her lifetime. Since Jane Doe needs to see the pediatrician in the first days and weeks of life, it will be necessary to provide health

insurance information for her. Jane Doe's DID™ card will already start to be used. The DID™ card is brought to the Insurance Company or to the home computer to link to the insurance company website by Jane Doe's mother. The card is placed in a reader with special contacts between the card and the reader which are only available for "INSURANCE-HEALTH" use. A digitally encrypted picture of Jane Doe, her mother and her father appears on the linked computer screen or LCD monitor at the insurance company. Jane Doe's mother places her thumb into the biometric sensor attached to the reader. The biometric print confirms that this is Jane Doe's mother and Jane Doe is the owner of the DID™ card. Jane Doe's information needed for insurance processing is then downloaded onto the database of the insurance company. The insurance company then downloads all needed insurance information for Jane Doe. The transaction ends . Jane Doe's first stop with her DID™ card is at the doctors office. She enters the office and presents the DID™ card to the office receptionist who places it in a reader. Jane Doe's photo, as well as her mothers and fathers appears on the LCD screen. Jane Does mothers fingerprint is entered via the attached biometric sensor(and retinal biometric as well). The receptionist verifies this is Jane Doe and her mother. The insurance information is then entered via USB port into the database of the doctors office. The exact time and place of the visit are stamped on Jane Doe's DID™ card via unique GPS technology. The "MEDICAL" portion of the card is accessed . The doctor records his findings. The uniquely placed pins only allows certain portions of Jane Doe's DID™ card to be read by the doctors office. The doctor then records his information from today's visit and downloads it onto the card. A typical entry may be as follows: *Jane Doe, age 2 weeks. Brought in by mother for well baby initial visit. Infant is healthy.*

Return in 2 weeks. May 6th 2003, 1248 hours, 394 Old Country Rd. Garden City N. E 11 53 0 and Jane Doe biometric downloaded to the doctor's record or medical database.

[0064] Jane Doe's subsequent visits can be recorded in a similar fashion. A detailed record of her allergies can be recorded. Her immunizations can be recorded. All her medications can be recorded. If she moves to another state, her DID™ card with all of her information can go with her. If the doctor prescribes medication for her, the prescription can be accurately read from her DID™ card in the pharmacy's reader. Drug interactions can be found before Jane Doe is harmed. Potential allergic reactions can be thwarted. Software which links the medication with the Insurance company formulary can save both Jane Doe and her insurance company money.

[0065] As Jane Doe grows her biometric information is updated on a yearly basis. Her medical history is documented. All of her immunizations are kept. Any trip to the emergency room is recorded for all of her doctors to see. Complete with date and time entered permanently into the record. Any visit Jane Doe had to the dentist office is also documented. Her dental x rays are added to her DID™ card for storage under the compartment labeled "DENTAL".

[0066] At the age of 12, Jane Doe is going to go on a family vacation to Europe. She must now get a passport to travel. This is perfect for her DID™ card. Jane Doe presents her DID™ card to the passport authorities in the U.S. Her digital photo appears on the screen after the card is placed in its reader. The reader cannot see any sections labeled "MEDICAL" or "DENTAL" to help secure Jane Doe's privacy. Nor can the reader see "INSURANCE HEALTH". Special contacts on the reader will allow certain transactions for this agency. A special section called "TRAVEL" appears on the screen. This only

occurs after Jane Doe's fingerprint and retinal scan document that this is Jane Doe's DID™ card. Passport information is downloaded onto the card. The information is stored in the databank of the agency for future use if needed. Jane Doe is now ready for her travel to Europe. Her parents have already purchased the tickets over the internet and downloaded them onto her DID™ card. Of course her biometric authorization was needed to download the ticket from her home computer with attached home reader with special contacts. She now only has to present her DID™ card at the airport with her biometric confirmations to board the plane and enter the European Union countries.

[0067] Jane Doe brings her DID™ card to the local DMV. Her identity is verified through the process she has been using her entire life to this point. Her photo is updated . She is given her drivers license which is downloaded directly onto her card. The DMV also adds her car registration and auto insurance information. These are in unique portions of her card known as "AUTOMOBILE-LICENSE", "INSURANCE-AUTOMOBILE", and "AUTOMOBILE-REGISTRATION" These portions can be read in the future by the DMV and local authorities. Any legal convictions or license restrictions will be seen here. Organ donor information can also be obtained. (This information may include the medical data needed for a national matching program to help hospitals communicate faster and find organ matches faster in the event of sudden death- this can be done through interfacing the card with the hospitals computer and national databanks. The card can have things like blood type and HLA matching etc.) All of this information is stored in the databanks of the DMV, which can be linked to hospitals.

[0068] One day, Jane Doe loses her DID™ card. She is not worried. She knows that no one can use her card due to the biometric encryption and the sensors needed for the card

to work. She then logs onto her computer at home and via the Internet uploads all of her information onto a new DID™ card, including information from . DMV, doctor or dentist, etc.. She is identified by her biometric data utilizing both a retinal scan, fingerprints, and stored photo. She may wish to keep two DID™ cards in case one is lost in the future. The process of replacing the information is simple and straight forward. Jane Doe is able to replace each compartment as it is needed. The fact that no one place holds all of her information protects her privacy.

[0069] Jane Doe became ill one day. She visited her new doctor. The doctor downloaded all of Jane Doe's history onto his database. He examined Jane Doe and decided she needed several medications. Jane Doe was not feeling well enough to go to the pharmacy to fill her prescription. Now she realized how elderly people that cannot get around much must feel. The doctor downloaded the prescriptions to the DID™ card. The time and place stamp was entered automatically by the DID™ card system. When Jane Doe returned home, she went to her Desktop computer. She placed her DID™ card in it's HOME USE ONLY reader which is connected to her computer. She placed her fingerprint on the biometric sensor and the computer confirmed she was the owner of the DID™ card. She downloaded the prescription which was sent electronically to her pharmacy. She added special instructions that said "please deliver" . The pharmacist also received Jane Doe's insurance information, allergies, and medical condition. He also received "other medications" notification to compare. The medication the doctor prescribed was not covered by the formulary of Jane Doe's insurance. An alternative was suggested by the preprogrammed software and confirmed with the doctor. Both Jane Doe

and her insurance company saved money, and Jane Doe was conveniently resting at home when her medications arrived.

[0070] There are numerous other possible uses as well, such as:

Jane Doe gets working papers;

Jane Doe opens a bank account;

Jane Doe gets her first credit card;

Jane Doe uses her DID™ card to cast her first electronic vote online;

Jane Doe goes to college and needs an ID card to get into the clubs and bars;

Jane Doe gets a job and her company uses DID™ cards for security;

Jane Doe juggles all of life's events using- her DID™ card for business, Personal ,travel, security, medical, and dental.

[0071] After a full and happy life. At the end of 99 years, Jane Doe dies. Her DID™ card is sent to the Social Security Administration after the Death Certificate has been downloaded. The SSA records Jane Doe's death and discontinues benefits.

[0072] In accordance with various aspects of the embodiments of the present invention, an example encompasses a lightweight, easily carried memory identification card for recording information and controlling access to this information. The memory card includes a file system of electronic files on the card, which are automatically detected and recognized by selected authorized readers. The file system is organized so that stored electronic files appear in separate and distinct compartments in the card, so that only authorized preselected readers have access to particular compartments.

[0073] Biometric identifying information is imprinted in the card, so that no data can be transferred unless there is a biometric match between a reader and a person assigned to

the card and who possesses the card. Biometric identifying information can be a thumbprint, fingerprint, digital face image, retinal image, voice recognition or any others known to those skilled in the art of biometrics, such as DNA sampling. One exemplary device suitable for fingerprint authentication performs both a fingerprint match and pulse detection on the finger itself

[0074] The memory identification card where desired can also have each compartment requiring a different unique pin code for access thereto. The separate compartments of the memory card may include a compartment containing, for example, medical information relating to the assigned user of the card, wherein the medical information is accessed only by a preselected memory card reader having the unique pin code assigned to the compartment having the medical information. In this manner, the medical information cannot be accessed by other providing institutions, such as banks or government agencies.

[0075] The memory identification card can also have a single chip Global Positioning System (GPS) engine, to identify where the card is being used.. In certain embodiments, the GPS engine is activated and powered by the memory card reader. In one embodiment the memory card does not need a separate power source, as the GPS information is revealed from flash memory when the card is inserted within the reader.

[0076] In another embodiment, the memory identification card has a power source, such as a battery. In one example, the battery may comprise a lithium cell adapted to be recharged by a preselected card reader. Such a battery-powered memory identification card can therefore be enhanced, such as with a microprocessor, RF receiver, and RF transmitter, for receiving and transmitting wireless telecommunications.

[0077] The memory identification card may also display a photo image of the person assigned to the card. In connection therewith, in one embodiment the memory identification card contains in a compartment a digitized photo image of the person assigned to the card, so that the exterior of the card will always bear the internally digitized image. A forger of the image on the exterior of the card will not be able to use the card. In addition, for fraud prevention, one of the compartments may contain biometric identifying information about the assigned user of the card.

[0078] The memory identification card also may have a button for initiating a call, such as to 911, and sending a prerecorded message with a request for emergency medical or other assistance. Such an embodiment can also provide the location of the memory identification card.

[0079] The memory card may also have the capability to be integrated with an apparatus for taking, storing and transmitting digital images, such as a digital camera.

[0080] Moreover, the memory identification card may have a an integrated or detachable memory stick/chip adapted to be programmed to record and document any disruption or removal of the card from an authorized user system.

[0081] As an alternate feature, the memory card may have a recorder integrated or attached to the card for storing real time voice data into the memory. In addition, security can be included to restrict access to the stored information, for example, wherein the recorded voice data can only be played back by access to a preselected reader.

[0082] In addition, the memory card can include an automatic voice notebook, wherein the card is embedded with a real-time clock for time stamping recorded voice segments.

[0083] Further, when the card has the recording capabilities, the recorder can have a connector to interface with a preselected reader, having the capability to playback the data signals stored on the memory identification card.

[0084] In certain embodiments, the memory identification card is part of a system for storing information unique to a particular person and using this information, for example, for identification, medical, security, insurance, entertainment, hospitality, financial and law enforcement purposes. Such embodiments may include one or more of the following features:

a) a central establishment for collecting and storing the information;

b) lightweight, memory card to be carried by the person for recording information downloaded from the actual establishment, wherein the card includes:

i) a file system of electronic files on the card which are automatically detected and recognized by selected readers, and the file system is organized so that stored electronic files appear in separate and distinct encrypted compartments; and

ii) biometric identifying information on the card so that no data can be transferred unless there is a biometric match between a reader and a person assigned to the card who possesses the card; and

c) preselected card readers programmed to extract information from the memory card from specific compartments, wherein each preselected reader has a unique pin code associated with a particular compartment on the memory identification card, so that a preselected reader can only extract information from a compartment for which the preselected reader has the proper pin code associated with that compartment.

[0085] Embodiments of the present invention also include a method of verifying the identity of, and extracting information about a person. In an exemplary embodiment, the person carries a memory card in which is stored identifying biometric information about the person, wherein this information is preferably stored in a compartment separate from other compartments on the card. The person submits the memory card to be scanned by a reader for identifying purposes, and the card reader has a unique pin code, which allows access to the encrypted compartment on the card.

[0086] Thereafter, an operator of the card reader compares the accessed biometric information with biometric information taken directly from the person having the memory identification card.

[0087] In addition, the memory identification card may contain other encrypted compartments, each of which includes a different bundle of information, such as medical, security, insurance, entertainment, hospitality, financial, travel, general business and law enforcement purposes, to name a few, and each compartment may further have a different unique pin code for access thereto.

[0088] It is further noted that other modifications may be made to the invention, within the scope of the approved claims. Accordingly, it is intended that the invention not be limited to the specific illustrative embodiments, but be interpreted within the full spirit and scope of the appended claims and their equivalents.